Technical Cybersecurity

The Path to APT

Fast, Complex

At this point things are moving more quickly

- We have more malware appearing
- It's more functional, more complex
- Combining malware and hacking
- Nation-state involvement
- Moving away from companies to larger targets

Infection Vectors

Social Engineering

- Common today, Kevin Mitnick started this approach
- Used to gain credentials and information

Phishing & Spearphising

- Combine malware with hacking approaches
- Multi-payload installations
- Interactive capabilities

New Targets & Techniques

2005: Sony rootkit

- Installed via CDs by Sony

2007: Storm Botnet

- Infects over 1M computers

2009: Stuxnet

- Uses malware to attack SCADA systems

What’s next?